IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) An internet service provider (ISP) Virtual Private Network (VPN) network comprising:

a plurality of edge routers;

a plurality of core routers adapted to allow communication between said plurality of edge routers;

a VPN application in communication with a first one of said plurality of edge routers, said VPN application having a first IP address; and

a black-hole router in communication with said plurality of core routers, said black-hole router adapted to inject a second IP address into said ISP VPN network, said second IP address comprising:

a same IP address as the first IP address;

a higher preference value than said first IP address; and

a community value such that when said second IP address is injected, a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router.

2. (Previously Presented) The ISP VPN network of claim 1, wherein said ISP VPN network is a Multiprotocol Label Switching Virtual Private Network (MPLS VPN).

3. (Previously Presented) The ISP VPN network of claim 1, wherein said black-hole router injects said second IP address in response to a Distributed Denial of Service (DDoS) attack on said VPN application.

4. (Previously Presented) The ISP VPN network of claim 1, wherein said

community value is changed in real-time by said black-hole router.

5. (Previously Presented) The ISP VPN network of claim 1, wherein said ISP VPN network utilizes one or more dynamic routing protocols in combination with a community-based route filtering to propagate the injected second IP address to said plurality of edge routers.

6. (Previously Presented) The ISP VPN network of claim 1 wherein when said selected second number of edge routers directs VPN traffic, addressed for said first IP address, to said black-hole router, said black-hole router is adapted to receive such VPN traffic as black-holed-traffic, said black-hole router adapted to analyze said black-holed traffic in order to determine a ratio of attack traffic to legitimate traffic.

7. (Previously Presented) The ISP VPN network of claim 1, further comprising at least one route reflector, each one of said at least one route reflector being connected to a different set of edge routers from said plurality of edge routers, said at least one route reflector being adapted to update said plurality of edge routers with route instructions, such route instructions including said injected second IP address.

8. (Previously Presented) An internet service provider (ISP) network comprising:

a plurality of edge routers;

an application in direct or indirect electrical communication with a first one of said plurality of edge routers;

said application having a first IP address such that Virtual Private Network (VPN) traffic addressed for said first IP address and entering said ISP network at any one of said plurality of edge routers, is routed to said application;

a black-hole router; and

a router adapted to inject an instruction into said ISP network, such that

one or more select edge routers redirect VPN traffic, which is addressed to said first IP address, to said black-hole router, wherein said injected instruction comprises a routing instruction having a same IP address as said first IP address, but with a higher preference value than said first IP address and having a community value.

9. (Canceled)

10. (Previously Presented) The ISP network of claim 8, wherein said ISP network is a Multiprotocol Label Switching (MPLS) VPN network.

11. (Original) The ISP network of claim 8, wherein said router and said black-hole router are the same device.

12. (Original) The ISP network of claim 8, wherein said injected instruction is a Border Gateway Protocol (BGP) routing instruction.

13. (Previously Presented) The ISP network of claim 8, wherein said black-hole router is adapted to receive redirected traffic from said one or more select edge routers and to determine a ratio of attack VPN traffic to legitimate VPN traffic found in said redirected traffic.

14. (Previously Presented) The ISP network of claim 8, wherein said router injects said instruction when said application is experiencing a Distributed Denial of Service (DDoS) attack.

15. (Previously Presented) A method of managing a Distributed Denial of Service (DDoS) attack on an application within an internet service provider (ISP) network, said application having a first IP address, said method comprising:

injecting a Border Gateway Protocol (BGP) routing instruction into said ISP network when said DDoS attack is occurring, said BGP routing instruction

comprising a second IP address having a same IP address as said first IP address, but with a higher preference value than said first IP address and having a community value;

redirecting, at one or more selected edge routers, VPN traffic addressed for said second IP address to a black-hole router; and

directing, at one or more other edge routers, VPN traffic addressed for said first IP address to said application that is experiencing said DDoS attack.

16. (Previously Presented) The method of claim 15, wherein said ISP network is a Multiprotocol Label Switching (MPLS) VPN network.

17. (Original) The method of claim 15, further comprising:

receiving, at said black-hole router, said redirected VPN traffic; and

determining an amount of attack traffic therein.

18. (Previously Presented) The method of claim 15, further comprising changing, in real-time, a number of said one or more selected edge routers that are redirected.

19. (Previously Presented) The method of claim 15, wherein said injecting said BGP routing instruction into said ISP network is done by providing said BGP routing instruction to a route-reflector for disseminating said BGP routing instruction to other route reflectors within said ISP network.